III. REMARKS

1. Claims 33-44 are amended.

2. Claims 2-4, 16-25 and 33-45 are not unpatentable over Kaydyk in view of either Ginter or Watanabe under 35 USC §103(a). The claims are amended to recite that the content packet is "device specific." This is not disclosed or suggested by the proposed combination of references. In order to avoid the necessity to restate the prior arguments, the arguments raised in the prior response are incorporated herein by reference in their entirety.

The Examiner takes "Official Notice" that a "device specific content package" is common and well known in the prior art with reference to network protocols. This position is respectfully traversed and the Examiner is requested to provide an evidentiary basis for the official notice in view of Applicant's comments and disqualification of Yianolos et al. ("Yianolos") (US 2001/0056533) below.

Although the Examiner refers to Yianolos in support of the Official Notice, Applicant respectfully submits that the authentication referred to by the Examiner is not the same as having a content packet that contains some other kind of device specific contents, and which can be loaded and installed in a device for use, as is claimed and described by Applicant. For example, referring to the paragraph starting on page 15, line 24 of Applicant's specification:

> The wireless communication devices 5a, 5b, 5c are equipped with content loading means, such as a content packet loading and installation application which can be run in connection with the control unit 34 of the wireless communication device. By means of the content loading means, the user can load and install content packets in the memory means of the wireless communication device 5a,

16

5b, 5c. Furthermore, these content loading means comprise means for decryption, if necessary. The user can start this application in a way known as such, by selecting, for example from (shortcut) icons referring to applications on a display device, an icon intended for this purpose, from the menu functions of the wireless communication device, or in another way known as such. By means of the content packet loading and installation application, the user can preferably search for the content packet on the basis of key words, classification, etc., download content packets in the wireless communication device 5a, 5b, 5c, as well as possibly also pay for the content packet by means of a data network (block 604)." (Emphasis added)

On the other hand, Yianolos relates to a computer platform that provides control features to allow for the protection of intellectual property rights and prevent malfunctioning of the platform. The platform uses 1) a secure operating system including a secure memory management system, 2) public key encryption, 3) data authentication through digital signatures and 4) application/data approval through a flexible access policy through the use of object handlers and an application program approval process. Through these four control features, the platform provides the ability to control access to data and minimize the effects of computer malfunctions. (see Abstract)

Data authentication is explained in paragraph [0019] of Yianolos as follows:

> Data authentication entails the ability of verifying the author and title of data to ensure that <u>the data is properly authored and has not been tampered with</u> from the time of creation by that author to the receipt by the platform. (Emphasis added)

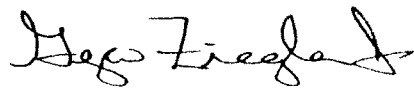Further, paragraph [0043] of Yianolos states:

> To authenticate the application program or object file, the first step 501 is to decrypt the encrypted data with the computer platform's private decryption key. After the data has been decrypted, the decrypted data should consist of the data packet and the digital signature. The next steps are to recreate the hash value of the data packet 503, and obtain the output from the publicly known signature verification algorithm 505. If the hash values do not match, then the data is erased from memory.

The authorization of Yianolos relates to verifying the data contained in the data packet. The authorization of Yianolos is not related to "device specific" content components which can be run in a device. Claims 33, 35 and 43 recites *providing information required by the wireless communication device to run the at least one device specific content component.* The feature of providing information needed to run the at least one device specific content component clearly distinguishes Applicant's claimed subject matter from the authorization system of Yianolos.

The authorization and the digital signature of Yianolos are not analogous to running a content component. Therefore, the Applicant respectfully submits that a "device specific content packet" as recited in the claims is no common and well known in the prior art in reference to network protocols, as is suggested by the Examiner. Thus, the claims are patentable over the combination of cited references.

The Commissioner is hereby authorized to charge payment for a 3-month extension of time, together with any other fees associated with this communication or credit any over payment to Deposit Account No. 16-1350.

Respectfully submitted,

_____
Geza C. Ziegler, Jr.
Reg. No. 44,004
Perman & Green, LLP
425 Post Road
Fairfield, CT 06824
(203) 259-1800
Customer No.: 2512

<u>22 July 2008</u>
Date